

In the Claims

Pursuant to 37 C.F.R. § 1.121(c)(1), applicants set forth amendments to claims 32 and 35 by rewriting claims 32 and 35 with all changes, adding new claims 36 - 43, and canceling claim 31. Also, applicant includes all pending claims, whether amended or unchanged, for the convenience of the Examiner.

1. A traffic management system for use in conjunction with packet data, said system operative for passing data packets there through, said system comprising:
means for reviewing certain parameters of data which is flowing into said system; and
means for remembering for a period of time said reviewed certain parameters in conjunction with each received packet.
2. The traffic management system of claim 1 further including:
means operative upon attainment of packet flow volume into said system reaching a certain level for temporarily storing certain subsequently received packets in accordance with selective remembered parameters of previously received packets.
3. The traffic management system of claim 2 wherein said certain level is user controlled.
4. The traffic management system of claim 2 wherein said certain level includes a plurality of levels, wherein the attainment of each successive level results in a more stringent application of said remembered certain parameters.
5. The traffic management system of claim 2 wherein said temporary storing means including a cache and a data storage, said data storage used when said cache is full.

6. The traffic management system of claim 1 wherein said remembered parameters include one or more of: a sender's address; a prior trouble-causing address; a notice of a potential trouble address; amount of data transmitted from a particular address in a period of time; number of packets arriving from a particular address in a period of time; an address' domain name; date of initial encounter with an address; date of latest encounter with an address.

7. The traffic management system of claim 6 further including:
means operative upon attainment of packet flow volume into said system reaching a certain level for temporarily storing certain subsequently received packets in accordance with selective remembered parameter of previously received packets; and

wherein said certain level includes a plurality of levels arranged in a sequence, and wherein as the sequence of levels gets closer to an absolute maximum data flow rate more and more of said remembered parameters are included as a basis for said determination to temporarily store a particular packet.

8. The traffic management system of claim 7 further including means for arbitrarily selecting packets for temporary storing when said data flow rate reaches its maximum capacity.

9. The traffic management system of claim 2 further including means for retrieving said temporarily stored data packets when traffic flow into said system falls below said certain level; and

means for putting said retrieved data packets through said system.

10. The traffic management system of claim 9 wherein said retrieving means includes means for retrieving packets in an order based upon why said packets had been stored.

11. The traffic management system of claim 2 further comprising means for dynamically displaying information pertaining to temporarily stored ones of said data packets.

12. The traffic management system of claim 11 further comprising means for transmitting said display information to a remote location.

13. The traffic management system of claim 11 wherein displaying means includes means for displaying data selected from the list of; prioritized packets in PTS, user overrides of prioritized stored packets, threshold limits reduced thereby automatically releasing stored packets.

14. A data network monitoring system comprising:
at least one data sniffer;
a temporary storage device;
a processor for performing data throughput measurements on data passing through said system; and

said processor further operative for diverting to said temporary storage device selected data entering said system, said selected data controlled in part by information obtained from said data sniffer and from said throughput measurement means.

15. The data network monitoring system of claim 14 wherein said system further comprises a store of data having undesirable characteristics, and wherein said processor operates to compare said store of undesirable data with data obtained from said data sniffer.

16. The data network monitoring system of claim 14 wherein said processor increases the number of said selected packets so as to maintain system throughput at or below a maximum number, where said maximum number is below the limits of the data transmission media entering said system.

17. The data network monitoring system of claim 14 further comprising means operable upon a determination that the data throughput through said system is below a certain limit for allowing certain ones of said diverted data to pass through said system.

18. The data network monitoring system of claim 14 further comprising a display for displaying in real time certain parameters pertaining to system operation.

19. The data network monitoring system of claim 14 wherein said parameters are selected from the list comprising: Preset Threshold Limits; Bandwidth Capacity; Allowed IP Addresses; Disallowed IP Addresses; and Prioritized Packets.

20. The method of controlling a traffic management system, said method comprising the steps of:
reviewing certain parameters of data packets flowing into said system;
remembering for a period of time said reviewed certain parameters in conjunction with each received data packet; and
upon attainment of packet flow volume into said system reaching a certain level, temporarily storing certain subsequently received packets in accordance with selective remembered parameter of previously received packets.

21. The method of claim 20 wherein said certain level is user controlled.

22. The method of claim 20 wherein said certain level includes a plurality of levels, wherein the attainment of each successive level results in a more stringent application of said remembered certain parameters.

23. The method of claim 20 wherein said remembered parameters include one or more of: a sender's address; a prior trouble causing address; a notice of a potential trouble address; amount of data transmitted from a particular address in a period of time; number of packets arriving from a particular address in a period of time; an address' domain name; date of initial encounter with an address; date of latest encounter with an address.

24. The method of claim 23 wherein said certain level includes a plurality of levels arranged in a sequence, and wherein as the sequence of levels gets closer to an absolute maximum data flow rate more and more of said remembered parameters are included as a basis for said determination to temporarily store a particular packet.

25. The method of claim 24 further including the step of:
arbitrarily selecting packets for temporary storing when said data flow rate reaches its maximum capacity.

26. The method of claim 20 further including the step of:
retrieving said temporarily stored data packets when traffic flow into said system falls below said certain level.

27. The method of claim 26 further including the step of:
putting said retrieved data packets through said system.

28. The method of claim 20 further comprising the step of:
dynamically displaying information pertaining to temporarily stored ones of said data packets.

29. The method of claim 28 wherein said displaying step includes:
transmitting said display information to a remote location.

30. The method of claim 28 wherein said displaying step includes
displaying data selected from the list of; prioritized packets in PTS, user overrides of prioritized stored packets, threshold limits reduced thereby automatically releasing stored packets.

31. This claim canceled.

32. (AMENDED) A data flow control system for preventing an enterprise data processing system from being overloaded with data requests directed to said enterprise system from sources external to said enterprise system, said data flow system comprising:

a gateway for accepting data directed to said enterprise system from any said external source;

a data monitoring circuit for observing selected portions of certain data directed to said gateway, and

A² a delay path operable when the amount of data currently being handled by said enterprise system reaches a certain threshold for temporarily removing selected data which is directed to said enterprise system away from enterprise system.

33. The system of claim 32 wherein the exact ones of said data which are temporarily removed are selected under control of information provided by said data monitoring circuit.

34. The system of claim 32 wherein said certain threshold has gradations and wherein the amount and types of data that are temporarily removed operate in proportion to said gradations.

35. (AMENDED) A method for preventing data from flowing beyond a particular point faster than the handling capability associated with that point; said system comprising the steps of:

A³ remembering certain parameters of data passing said particular point; and
preventing selected data from passing said particular point when the data handling capability associated with that point reaches a preset limit, said preventing step relying, in part, on said remembered parameters pertaining to data previously passing said particular point.

36. (NEW) The method of claim 35 wherein said preventing step includes the step of storing said selected data for a period of time.

37. (NEW) The method of claim 36 further including the step of selectively sending at least portions of said stored data to pass through said particular point.

38. (NEW) The method of claim 35 wherein said preset limit is selected from the list of:

prior trouble causing addresses;

a notice of potential trouble addresses;

an amount of data transmitted from a particular address in a period of time;

number of data packets arriving in a period of time;

number of data packets arriving in a period of time from a particular sending address;

identified questionable changes in a specific sender address.

39. (NEW) The method of claim 35 further including the step of sending messages to an external location indicating the steps of data flow through said particular point.

40. (NEW) The method of claim 2 wherein said data is flowing into said system from a public network and directed to a particular address on said network.

41. (NEW) The method of claim 2 wherein said data is flowing into said system from a particular address on a public network, said data destined for an address on said public network.

42. (NEW) The data network of claim 14 wherein said data which is diverted by said processor may originate at a specific site and destined for a public network or may originate at a location connected to the public network and destined for said specific site.

43. (NEW) The method of claim 20 wherein said data packets flowing into said system may come from a public network or may come from a specific system.